IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.: 1:18 CR 22
	)	
Plaintiff,	)	JUDGE SOLOMON OLIVER, JR.
	)	
v.	)	
	)	
PHILIP DURACHINSKY,	)	GOVERNMENT'S RESPONSE IN
	)	OPPOSITION TO DEFENDANT'S
Defendant.	)	MOTION TO SUPPRESS

Now comes the United States of America, by its counsel, Justin E. Herdman, United States Attorney, Daniel J. Riedl, Om M. Kakani, Assistant United States Attorneys, and Brian L. Levine, Senior Counsel for the U.S. Department of Justice, and hereby opposes Defendant Philip Durachinsky's Motion to Suppress.

I. INTRODUCTION

Durachinsky has confessed to the ultimate violation of privacy—infecting thousands of computers with a virus in order to secretly turn on the cameras and microphones on those computers so that Durachinsky could watch, record, and archive unwitting adults and children in a state of undress and/or engaged in sex acts. Durachinsky now argues that all the evidence from his laptop (and subsequent confession) should be suppressed because his rights were violated when the United States seized his laptop on an exigent basis and obtained a warrant to search the laptop immediately thereafter. Durachinsky's motion is without merit and should be denied because (1) his laptop was properly seized pursuant to the exigent circumstances exception to the warrant requirement and searched pursuant to a warrant signed less than six hours later; (2) the United States acted in good faith at all times; and (3) the inevitable discovery doctrine applies.

II. BACKGROUND

A. FRUITFLY MALWARE

Durachinsky created and propagated his own malware, which was later named "Fruitfly" by security researchers. "Fruitfly" malware was unusual because it was primarily used to infect computers running Apple's macOS X operating systems in addition to Microsoft Windows computers. Once a computer was infected, the operator of the malware could gain unauthorized access to documents, photos, videos, and other files on the infected computer. Further, the Fruitfly malware could be used (and was frequently used) to covertly turn on the camera and microphone on an infected computer to record and transmit photographs and videos of innocent victims (including children) during their most private moments. Finally, some versions of the Fruitfly malware could be used to record users' keystrokes as they typed, allowing Durachinsky access to their written words and passwords. Thousands of computers were infected with the Fruitfly malware, resulting in the illicit and invasive recording and transmission of millions of photographs and videos of victims.

Once a computer was infected with the Fruitfly malware, Durachinsky would provide instructions to the infected computer, such as "turn on your camera and microphone and begin recording." Durachinsky programmed the malware to reach out via the internet to certain domain names (e.g., tmp1.hopto.org, eidk.hopto.org, etc.) in order to receive his instructions and then send back victims' personal information to him. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 309-10). The victims' computers would then automatically reach out to a Domain Name Server ("DNS") to determine the IP address associated with the domain name provided by the malware. The victims' computers would then automatically connect to that IP address and receive instructions from Durachinsky, and in many cases, send personal information from the victims' computers to him.

B. THE FBI'S INVESTIGATION BEGINS

The FBI's investigation into the Fruitfly malware began on or about January 5, 2017, when Case Reserve Western University ("CWRU") contacted the FBI regarding a newly discovered intrusion on the CWRU network. (Id., PageID 309). CWRU identified over 100 computers on their network infected with the Fruitfly malware. (Id.).

In the course of CWRU's internal investigation, CWRU determined that an IP address involved in malware communications was the same IP address that one of CWRU's alumni—Philip Durachinsky—used to log into the CWRU network. (Id., PageID 310). Philip Durachinsky was previously known to CWRU, having been referred to student affairs for "password cracking" the CWRU network while a student. (Id.).

On January 12, 2017, the FBI served a subpoena on AT&T seeking subscriber information associated with an IP address identified by CWRU. (Id.). Records received from AT&T two days later revealed that the IP address resolved to a specific residential address in North Royalton, Ohio—the home of Durachinsky and his parents. (Id.).

In addition, domain names used by the malware to receive instructions (e.g., tmp1.hopto.org, eidk.hopto.org, etc.) were set to instruct infected computers to connect to the same IP address resolving directly to Durachinsky's home. (Id., PageID 309-12). The FBI's open source research also confirmed that Durachinsky had the "particular technical knowledge" that would be required to create or manage the malware used by Durachinsky. (Id., PageID 311).

Between January 4 and 18, 2017, Durachinsky's victims began to "independently share infection data, interrogate compromised systems, and remediate networks." (Id.). "Due to this activity, some of which would have been detectable by [Durachinsky], the FBI was concerned that [Durachinsky] would become aware that the malware was detected and remediated, and start to hide his tracks." (Id.). Consistently, on or about January 13, 2017, Durachinsky changed the

domain he was using to communicate with infected computers to point from his home to an IP address located in California. (Id., PageID 311-12). "The FBI interpreted this as a possible reaction to investigation activity by numerous intrusion victims." (Id.).

C. DURACHINSKY IS OUTED

On January 18, 2017, an article on a malware research website reported on the Fruitfly malware and identified (1) an IP address used by Fruitfly to communicate with infected computers that resolved to North Royalton, Ohio—the location of Durachinsky's home; and (2) a domain name that Fruitfly used to direct infected computers to connect to an IP address resolving directly to Durachinsky's home. (Id., PageID 312; Exhibit A at 2). On the same day, public reporting showed that Apple became aware of the Fruitfly malware and began the process of rolling out a patch to disable the malware. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 312; Exhibit A at 5). Thus, on January 18, 2017, both Apple and the malware research website had suddenly given increased attention to the Fruitfly malware, and publically provided information leading directly to Durachinsky's residence. "Given the above events, the FBI believed it was highly likely that the subject would determine that his malware was being widely detected, and attempt to destroy any technical evidence of his involvement." (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 312). Indeed, the fact that Apple was in the process of disabling the Fruitfly malware meant that it was soon unlikely to work anymore, making it more likely that Durachinsky would destroy everything related to the malware. Durachinsky now had everything to gain and nothing to lose by destroying his records.

Later that same day, the FBI discussed this matter with Department of Justice attorneys in the Northern District of Ohio and Washington, D.C. Based on these conversations, and believing the imminent destruction of evidence was likely, in the evening of January 18, 2017, while FBI agents were still in their offices, the United States contacted Magistrate Judge William H.

Baughman, Jr., the magistrate judge on duty, to inform him that they would be sending him a search warrant to sign late that night. Magistrate Judge Baughman provided the United States with instructions for reaching him at home.

D. THE EXIGENT CIRCUMSTANCES SEIZURE

Although the United States does not rely on any events that took place at Durachinsky's home to establish either probable cause or exigent circumstances, the events discussed below may be relevant to the issue of whether the manner of execution of the exigent circumstances seizure was reasonable. See infra p. 18.

At 10:00 p.m. on January 18, 2017, the FBI conducted a "knock and talk" at Durachinsky's home. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 312).[1] It is not disputed that "Defendant's parents indicated to the Government agents that they consented to some of the law enforcement agents entering the house, to the inspection of their computers, and allowed agents into the rooms in which their computers were situated." (R. 63: Motion to Suppress, PageID 262).[2]

---

[1] The Sixth Circuit has recognized a "knock and talk" as "a legitimate investigative technique at the home of a suspect or an individual with information about an investigation." United States v. Thomas, 430 F.3d 274, 277 (6th Cir. 2005) ("A number of courts, including this one, have recognized 'knock and talk' consensual encounters as a legitimate investigative technique at the home of a suspect or an individual with information about an investigation."); see also United States v. Lucas, 640 F.3d 168, 174 (6th Cir. 2011); United States v. Chambers, 395 F.3d 563, 568 n.2 (6th Cir. 2005) ("Courts generally have upheld [the knock and talk] investigative procedure as a legitimate effort to obtain a suspect's consent to search."), abrogated on other grounds by Kentucky v. King, 563 U.S. 452 (2011); Ewolski v. City of Brunswick, 287 F.3d 492, 504–05 (6th Cir. 2002) (concluding that it was reasonable to approach a suspect's home to attempt to learn more through consensual questioning).

[2] Defendant asserts that "an objective review of the circumstances at the time, reveal that [his parents'] 'consent' was *probably* not voluntary." (R. 63: Motion to Suppress, PageID 262 (emphasis added)). For this proposition, defendant relies primarily on United States v. Tatman, 397 F. App'x 152 (6th Cir. 2010). Tatman and the other cases cited by Durachinsky, however,

Mr. Durachinsky advised the FBI that his son was "very smart regarding computers," that he worked for a technology company, and that he only stayed at their home on weekends. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 312-13). Durachinsky's parents also told investigators that their son "got into trouble" for "breaking into" his high school's website, and "reading teachers' emails." (Id., PageID 314).

Mrs. Durachinsky advised the FBI that her son "had a laptop . . . which he remotes into from work." (Id., PageID 313). As Defendant notes in his motion, "Mrs. Durachinsky . . . went down the hallway and showed the FBI agents Defendant's computer room, which was his childhood bedroom, was used exclusively by Defendant, and which contained his laptop computer. . . . Mrs. Durachinsky opened the door, and pointed to an ACER Aspire laptop sitting on a desk." (R. 63: Motion to Suppress, PageID 240).

According to the FBI, at least one agent "noticed the laptop lid was slightly open and observed the mouse pointer was moving and the screen was updating." (Id.). Based on this

---

involved consent to *search* a house. Here, the government only relied on Durachinsky's parents' consent to *enter* the house (and the rooms to which Durachinsky's parents led the FBI). The seizure was made pursuant to exigent circumstances (not consent) and the search was undertaken pursuant to a warrant obtained six hours later (not consent). Moreover, in Tatman, the consenting party provided a sworn declaration stating that law enforcement told her that consenting to the search would "protect" her from being criminally charged and from "losing [her] home." Id. at 165. Defendant does not claim that the FBI made any improper promises or threats to gain entrance to the house here. Defendant only claims that his parents were a "naïve, older, law-abiding couple," that it was "late at night (10:00 p.m.), in the middle of winter" (R. 63: Motion to Suppress, PageID 250), that two men accurately identified themselves as FBI agents, accurately stated they were "conducting an investigation involving suspicious network activity originating from an IP address registered to their home," and that additional FBI agents entered later to assist. (Id., PageID 238-39). Defendant offers no evidence whatsoever (e.g., a declaration as in Tatman) to suggest the consent to enter the home was involuntary and cites no authority to suggest that seniors are unable to voluntarily invite law enforcement in at night or in the winter.

observation, the agent believed someone was remotely accessing the laptop. (Id.). Because Durachinsky claims that the FBI could only have seen activity on his laptop screen by opening up the screen, however, the United States assumes *arguendo* (for purposes of this motion only) that Defendant is correct and that the FBI identified activity on the screen only once it opened the laptop to check for encryption and to "preserve volatile data." See discussion infra pp. 16-17 n.7.

Mrs. Durachinsky attempted to contact her son at work and left him a message. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 314). The FBI then unplugged the power cord from the AT&T router "to prevent the remotely connected user from deleting information from the laptop." (Id.). The FBI checked for encryption and cell phone video and photos were taken of the laptop screen in order to preserve evidence. (Id.). It appeared that "a malware control panel" consistent with the Fruitfly malware was displayed on the screen. (Id.).

Shortly after the FBI unplugged the router, Durachinsky called home and his mother explained that the FBI was there and wanted consent to search his laptop. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 314-15). Durachinsky told investigators that he did not want to provide consent "due to a faulty power cord attached to the laptop" and because "some work files were present on the laptop." (Id.). The FBI told Durachinsky that it would be seizing the laptop due to exigent circumstances and would obtain a warrant. (Id.). Durachinsky "advised he was coming to the residence with some friends to discuss the matter." (Id., PageID 315).

The seizure occurred at approximately 10:55 p.m. (Id.). Because the United States had advised the magistrate judge that it would be submitting a late night search warrant prior to

arriving at Durachinsky's home,[3] the magistrate judge was able to sign the warrant at 4:40 a.m.—less than six hours after the seizure. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 305).[4]

A subsequent search of the laptop revealed that Durachinsky was using the Fruitfly malware to obtain and manage, and store files, personal information, photographs, and sound recordings of thousands of unwitting victims. Indeed, Durachinsky used his malware to secretly produce child pornography and illicit images from unknowing children.

Durachinsky was arrested on a complaint on January 25, 2017. On April 28, 2019, Durachinsky moved to suppress the evidence from the January 18, 2017 seizure, and any so-called "derivative" evidence (including his confession).[5]

---

[3] Drafting a Rule 41 search warrant and affidavit in a complex computer crime case typically requires significant collaboration between both agents and prosecutors, and generally takes hours, if not days to prepare.

[4] Defendant's expert report implies that the FBI might have searched Durachinsky's laptop prior to the warrant being issued. (R. 63-1: Exhibit A to Defendant's Motion to Suppress, PageID 267). In fact the "file system mounted" events referenced by Durachinsky's expert do not reflect actions taken by the FBI. Instead, they likely represent automated processes occurring on Durachinsky's computer or commands or instructions he had previously entered into his computer. These processes occurred because the FBI kept Durachinsky's laptop powered on until after the warrant was issued and until the laptop could be subsequently imaged (i.e., copied). This is a recommended practice to reduce the likelihood that evidence will become encrypted. The "bash history modified" entry on the system logs, reflected commands entered into the laptop by the FBI at Durachinsky's house, also in an effort to determine whether Durachinsky was using any type of encryption that would render his data inaccessible if his laptop was powered down or allowed to go into an inactive state. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 314; see also discussion infra at pp. 16-17 n.7). The FBI took no steps to review or search the laptop until the warrant was sworn out—only steps to prevent any data from becoming encrypted and to preserve volatile data.

[5] Because the United States is confident that the exclusionary rule does not apply at all to this seizure, it does not address whether so-called "derivative" evidence would also be properly excluded. (R.63: Motion to Suppress, PageID 258). In the unlikely event that the Court determines that the exclusionary rule does apply, the United States respectfully requests leave to separately brief the issue of "derivative" evidence and its exclusion.

III. ARGUMENT

A. THE SIX-HOUR SEIZURE OF DURACHINSKY'S LAPTOP WAS PROPER PURSUANT TO THE EXIGENT CIRCUMSTANCES DOCTRINE

The Fourth Amendment to the United States Constitution protects the people "against unreasonable searches and seizures." In general, warrantless searches and seizures are "per se unreasonable . . . subject only to a few specifically established and well-delineated exceptions." City of Los Angeles v. Patel, 135 S. Ct. 2443, 2452 (2015) (quoting Arizona v. Gant, 556 U.S. 332, 338 (2009). One of the exceptions is exigent circumstances, which applies where law enforcement authorities have probable cause to believe a container holds evidence of a crime, but the "exigencies of the circumstances" demand immediate seizure of the container pending issuance of a warrant to examine the contents. United States v. Place, 462 U.S. 696, 701 (1983).

In Illinois v. McArthur, 531 U.S. 326, 334 (2001), the Supreme Court upheld an exigency-based seizure based on reasoning wholly applicable to this case. In McArthur, a police officer temporarily seized the defendant's home until another officer returned with a warrant to search the home for drugs. 531 U.S. at 328-29. The Supreme Court observed that it "ha[d] found no case in which this Court has held unlawful a temporary seizure that was supported by probable cause and was designed to prevent the loss of evidence while the police diligently obtained a warrant in a reasonable period of time." Id. at 334. The Court concluded that the seizure did not violate the Fourth Amendment. See id. at 337. In particular, the Court found that (1) there was "probable cause to believe that [the defendant's] home contained evidence of a crime and contraband"; (2) "the police had good reason to fear" that evidence would be destroyed "before they could return with a warrant"; (3) "the police made reasonable efforts to reconcile their law enforcement needs with the demands of personal privacy"; and (4) "the police imposed the restraint for a limited period of time" that "was no longer than reasonably necessary

for the police, acting with diligence, to obtain the warrant." Id. at 331-33. As explained below, these four McArthur factors were also present in this case, and the temporary seizure of Durachinsky's computer while the FBI obtained a warrant did not violate the Fourth Amendment

1. The United States had probable cause to search any computer in Durachinsky's house prior to arriving at the house.

"The probable cause requirement . . . is satisfied if the facts and circumstances are such that a reasonably prudent person would be warranted in believing that an offense had been committed and that evidence thereof would be found on the premises to be searched." Greene v. Reeves, 80 F.3d 1101, 1106 (6th Cir. 1996) (quoting United States v. Besase, 521 F.2d 1306, 1307 (6th Cir. 1975)). Notably, there is no requirement that any person living or working in a "premises to be searched" be guilty of a crime or even associated with the crime—only that "evidence" of the crime is likely to "be found on the premises to be searched." Id.

In addition, the Sixth Circuit recently clarified that if there is "probable cause to believe that a crime has been committed by means of an object," such as a computer, "a magistrate may presume that there is a nexus between that object and the suspect's current residence, unless the affidavit contains facts that may rebut that presumption." Peffer v. Stephens, 880 F.3d 256 (6th Cir. 2018). In this case, not only had the FBI determined that their suspect, Durachinsky, resided in the home at issue, but the FBI also determined that the crime was committed through an IP address explicitly assigned to the internet router in Durachinsky residence.

Indeed, prior to visiting Durachinsky's house, the FBI had already received records from AT&T confirming that an IP address the Fruitfly malware was using to communicate resolved to Durachinsky's house. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 310). The Sixth Circuit has repeatedly held that where an IP address associated with online criminal activity resolves to a residence, there is probable cause to search the residence, including the

computers in the residence. See, e.g., United States v. Gillman, 432 F. App'x 513, 515 (6th Cir. 2011) (holding that a residential IP address "established sufficient nexus connecting the sharing of child pornography to [defendant's] residence and computer" and finding that the fact that "someone else could have accessed" defendant's home wireless network did "not negate the fair probability that child pornography emanating from an IP address will be found on a computer at its registered residential address."); United States v. Hinojosa, 606 F.3d 875, 885 (6th Cir. 2010) (holding that probable cause "would have justified the issuance of a search warrant" where "[p]rior to entering the residence, the officers had established that (1) videos and images involving child pornography were transferred to undercover agents from a specific IP address; (2) the IP address was registered to Defendant at a Lansing, Michigan, address; and (3) Defendant resided at the Lansing, Michigan, address."); United States v. Wagers, 452 F.3d 534, 539 (6th Cir. 2006) (finding "sufficient evidence to establish probable case" where "an IP address assigned by [a residential internet provider] to [defendant] was used to purchase" membership on child exploitation websites); see also United States v. Kinison, 710 F.3d 678, 684 (6th Cir. 2013) ("It makes sense under the flexible, common-sense approach to probable cause determinations, that where police have no 'inside scoop,' they would rely on other peripheral data, i.e. an IP address or email provider, to connect an alleged crime with a place to be searched.").

Here, however, the FBI had much more than just records from AT&T to connect the crime to Durachinsky's residence. First, CWRU independently determined that an IP address involved in Fruitfly communications was the same IP address that Philip Durachinsky—one of CWRU's alumni—was using to log onto the CWRU network to check his alumni email account. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 310). Further, on the day of the

seizure, an article on a malware research website reported on the Fruitfly malware and identified (1) an IP address used by Fruitfly that resolved to North Royalton, Ohio—the location of Durachinsky's residence; and (2) a domain name that Fruitfly used to instruct infected computers to connect to an IP address that resolved directly to Durachinsky's home. (Id., PageID 312; Exhibit A at 2). Thus, prior to the seizure, three different sources had independently identified IP addresses used by the Fruitfly malware—AT&T (in response to a grand jury subpoena), CWRU (based on its internal investigation), and the malware research website (based on its own research). AT&T identified the IP address as resolving to Durachinsky's residence. CWRU identified the IP address as being one used by their alum, Philip Durachinsky.

Second, CWRU also reported that Durachinsky had previously been referred to student affairs for "password cracking" the CWRU network while a student. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 310). "Although a defendant's criminal history is not dispositive, it is relevant to the probable cause inquiry." Wagers, 452 F.3d at 541 (citing United States v. Dyer, 580 F.3d 386, 392 (6th Cir. 2009)); see also Hogan v. Lewis Cty., No. 716CV1325LEKATB, 2018 WL 4689094, at *16 (N.D.N.Y. Sept. 28, 2018) (Slip Copy) (finding probable cause based, in part, on evidence that defendant had been "arrested" for engaging in "similar acts" in the past).

This information provided by CWRU suggested that developing malware to gain unauthorized access to computers was consistent with Durachinsky's skills, abilities, and modus operandi. The FBI's open source research further confirmed that Durachinsky had the "particular technical knowledge" required to create or manage the malware. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 311). See Dyer, 580 F.3d at 392 (search warrant

upheld where "information gleaned from the confidential informant in this case was corroborated by the officers' own observations and research.").

Third, the FBI had already confirmed that a domain name used by the Fruitfly malware to communicate directed victims to an IP address that resolved to Durachinsky's home. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 310-11). See, e.g., United States v. Richards, 659 F.3d 527, 532 (6th Cir. 2011) (upholding warrant where probable cause was based, in part, on the fact that defendant registered domains used to host child pornography in his name).

Thus, prior to January 18, 2017, the United States already had probable cause to believe that evidence of a crime would be found on computers at the Durachinsky residence, and would have obtained a search warrant before seizing Durachinsky's laptop, absent the exigency. Indeed, prior to the seizure, not only had attorneys from the Department of Justice confirmed that probable cause existed, but the United States had already informed the magistrate judge on duty that they would be submitting a search warrant late that night and received instructions on how to reach the magistrate judge at home.

2. Investigators reasonably believed that, absent a seizure of Durachinsky's computer, evidence would be destroyed.

In McArthur, the Supreme Court observed that seizure of the defendant's home was justified because police "reasonably believed that the home's resident, if left free of any restraint, would destroy that evidence." McArthur, 531 U.S at 337; see also United States v. Sangineto–Miranda, 859 F.2d 1501, 1511 (6th Cir. 1988) (the Sixth Circuit "has long recognized, along with many others, that exigent circumstances will be present when there is an urgent need to prevent evidence from being lost or destroyed.")

When deciding whether sufficient exigent circumstances existed to justify a warrantless seizure, the court must consider the "totality of the circumstances and the inherent necessities of the situation." Brooks v. Rothe, 577 F.3d 701, 708 (6th Cir. 2009) (citing United States v. Rohrig, 98 F.3d 1506, 1511 (6th Cir. 1996)).[6] "The inquiry focuses not on an officer's subjective intentions, but on whether an objectively reasonable officer *could have believed* that exigent circumstances existed." Brooks, 577 F.3d at 708 (emphasis added) (citing O'Brien v. City of Grand Rapids, 23 F.3d 990, 999 (6th Cir. 1994)). Here, investigators had an objectively reasonable basis for concluding loss or destruction of evidence was imminent.

On January 18, 2017, the day of the seizure, it was reported that Apple became aware of the Fruitfly malware and began the process of updating to the Mac operating system to disable the malware. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 312; Exhibit A at 5). This meant that not only had the Fruitfly malware just gained an enormous amount of visibility, but also that it was unlikely to work in the future—significantly reducing Durachinsky's incentive to maintain his Fruitfly operation.

That same day, an article on a malware research website detailed the Fruitfly malware, and publicly identified both a domain name resolving to Durachinsky's home in North Royalton, Ohio and an IP address also resolving to North Royalton, Ohio. (Id., see also Exhibit A at 2). In other words, there was now public reporting that the Fruitfly malware was communicating through a domain and IP address linked directly to Durachinsky. That meant that, if

[6] Such an inquiry that is at odds with a bright-line evidentiary requirement. Cf. United States v. Canipe, 569 F.3d 597, 601 (6th Cir. 2009) (noting that reasonableness of length of detention during traffic stop is not subject to a bright-line rule but focuses on the totality of the circumstances); United States v. Luqman, 522 F.3d 613, 616 (6th Cir. 2008) (observing that reasonable suspicion is judged by totality of the circumstances, not by bright-line rules).

Durachinsky had not already been identified by law enforcement, all that would be required for law enforcement to do so was to subpoena AT&T for the subscriber records (a step the FBI, in fact, had already taken). (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 310-11). Thus, it seemed highly likely to the FBI agents involved in the investigation that Durachinsky would destroy evidence of his crimes, particularly given that law enforcement believed that Durachinsky had recently moved his criminal infrastructure in response to less. (Id., PageID 311-12).

Indeed, extensive authority supports the common sense notion that when criminals believe they have been caught or are about to be caught, they often destroy evidence of their crime. See Kentucky v. King, 563 U.S. 452, 461 (2011) ("[I]n the vast majority of cases in which evidence is destroyed by persons who are engaged in illegal conduct, the reason for the destruction is fear that the evidence will fall into the hands of law enforcement."); see also United States v. Cruz, No. CR 18-1105 JB, 2019 WL 957108, at *43 (D.N.M. Feb. 27, 2019) (compiling cases for the proposition that "[c]ourts frequently uphold the likelihood of evidence's destruction when law enforcement officers . . . know that a defendant has become aware of law enforcement officers' interests in his or her activities or of their presence near the evidence.")

Durachinsky argues that the exigency exception applies only "when the police do not create the exigency" (R. 63: Motion to Suppress, PageID 257), but even if that were true, the FBI did not create the exigency. Here, based on information obtained by the FBI prior to entering Durachinsky's house, the FBI already had (1) reason to believe it was likely that Durachinsky or others would destroy the evidence if law enforcement did not seize it immediately; and (2) probable cause to search Durachinsky's entire home for devices that might contain evidence of the cybercrimes under investigation. See King, 563 U.S. at 462 ("Where . . . the police did not

create the exigency by engaging or threatening to engage in conduct that violates the Fourth Amendment, warrantless entry to prevent the destruction of evidence is reasonable and thus allowed.").

Nor did anything that happened in Durachinsky's house that night resolve the concern that evidence of a crime might be destroyed. To the contrary, the events at Durachinsky's house validated the concern. For example, when law enforcement arrived at the Durachinsky residence, it appeared that Durachinsky was remotely accessing his laptop and what was displayed on the screen appeared to be "a malware control panel" consistent with the malware under investigation. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 313-14; see also Exhibit B). Thus, it was possible Durachinsky was already in the process of destroying evidence.[7]

---

[7] Durachinsky's motion focuses on his argument that FBI agents must have "(1) enter[ed] Defendant's computer room without consent, and mov[ed] a chair that was blocking the view of the laptop computer, and (2) open[ed] the closed lid of the computer and look[ed] at the screen." (R. 63: Motion to Suppress, PageID 257; see also R. 63-1: Exhibit A to Defendant's Motion to Suppress). While that is contrary to the recollection of more than one FBI officer who was present, even assuming for the sake of argument Durachinsky was correct, it would not impact the legal analysis for this motion for two reasons:

First, before even entering Durachinsky's house, the government already had probable cause to search Durachinsky's entire house for digital devices that might contain evidence of the cybercrimes and had already committed to doing a temporary seizure based on exigent circumstances having nothing to do with anything that later occurred in Durachinsky's house. Consistently, before arriving at the residence, the government had already made arrangements with the magistrate judge to do a late night search warrant as soon as the laptop had been seized. Indeed, consistent with advice provided by the Department of Justice, law enforcement planned to and would have temporarily seized the laptop on an exigent basis even if the laptop had been completely powered off with nothing visible on the screen.

Second, even assuming *arguendo* that Durachinsky is correct that agents lifted the lid of his laptop or otherwise accessed the laptop before powering it down, that is a standard procedure for seizing any computer that is powered on. See Ovie Carroll, Challenges in Modern Digital Investigative Analysis, 65 US Attorneys' Bulletin, Jan 2017, at 27-28 (available online at www.justice.gov/usao/page/file/931366/download) (noting that "[w]ith the increased likelihood

After the FBI disconnected the router to prevent Durachinsky from destroying evidence, Durachinsky called the residence. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 314-15). Durachinsky would not consent to the FBI's search of the laptop and advised the FBI that "he was coming to the residence with some friends to discuss the matter." (Id., PageID 315). The seizure occurred at approximately 10:55 p.m. (Id.). A warrant was signed at 4:40 a.m.—less than six hours later. (Id., PageID 305).

Courts have doubted the wisdom of leaving the owner of easily-destructible evidence in possession of that evidence once the owner is aware that law enforcement is seeking a warrant. See McArthur, 531 U.S. at 332 (finding it reasonable for law enforcement to conclude that defendant suspecting an imminent search "would, if given the chance," get rid of contraband quickly). Indeed, the Sixth Circuit has said that "it is objectively reasonable to seize a container an officer has probable cause to believe contains evidence of a crime, rather than leave it unguarded in the hands of a suspect who knows that it will be searched." United States v. Bradley, 488 F. App'x 99, 103 (6th Cir. 2012) (finding officer's belief of exigent circumstances to be "objectively reasonable" because "[h]ad [police] left the laptop in [target's] possession, [target] could have attempted to destroy any computer files or the laptop itself.").

---

of encountering encryption," before powering down a computer, law enforcement should "check for signs of encryption" and "isolate and preserve the computer as it is when law enforcement first encounter it," including by "preserv[ing] volatile data"). Consistently, the search warrant noted that "[i]n order to preserve evidence," "[c]ell phone video and still shots were taken of the laptop screen" and FBI agents "entered commands on the ACER laptop to determine if there was encryption on the laptop" (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 314-15). Thus, the FBI would have discovered the malware control panel in short order, even under Durachinsky's version of events.

In short, defendant's forensic argument has no legal import.

In the present case, Durachinsky may not have been physically present at his home, but his parents were present. (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 312). Durachinsky was remotely accessing his laptop (id., PageID 313), and Durachinsky was made aware that the FBI wanted to search his laptop (id., PageID 314-15). See United States v. Campbell, 261 F.3d 628, 632-33 (6th Cir. 2001) (all that is required is proof of "someone" in the house who might destroy the evidence, whether defendant or a "third-party"); see also United States v. Saddler, 498 F. App'x 524, 529 (6th Cir. Sept. 4, 2012) ("it was objectively reasonable for the officers to believe that Saddler *or a third-party* might remove the evidence from inside the safe, take the safe from the scene, or otherwise tamper with it." (emphasis added)). Moreover, Durachinsky indicated to the FBI that he was not far from the residence and that "he was coming to the residence with some [unidentified] friends." (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 314-15).

3. The manner of execution was reasonable.

In McArthur, the Supreme Court also observed that the manner of seizing the defendant's house was reasonable: officers "imposed a restraint that was both limited and tailored reasonably to secure law enforcement needs while protecting privacy interests." McArthur, 531 U.S. at 337. As the Sixth Circuit has said, the court must "balance the interests by weighing the governmental interests being served by the intrusion against the individual interest that would be protected if a warrant were required." Saddler, 498 F. App'x at 529 (quoting United States v. Plavcak, 411 F.3d 655, 664 (6th Cir. 2005)).

a. Governmental Interest

Here, the government's interest in preserving the evidence on Durachinsky's laptop was strong. First, "[t]he government's interest in solving crimes is significant, of course, and the evidence seized was materially important to the investigation." Saddler, 498 F. App'x at 529.

Indeed, Durachinsky's laptop contained direct evidence of his use of malware to infect and control the victims' computers, as well as his own treasure trove of documents, photos, audio, and other files Durachinsky obtained from his victims' computers.

Second, the Supreme Court has repeatedly stressed that the government has an important interest "in protecting the well-being, tranquility, and privacy of the home." Carey v. Brown, 447 U.S. 455, 471 (1980); see also FCC v. Pacifica Foundation, 438 U.S. 726, 748 (1978). As the Supreme Court stated in Frisby v. Schultz, the government's interest in protecting the privacy of the home—the "last citadel of the tired, the weary, and the sick"—is "of the highest order." 487 U.S. 474, 484 (1988). Here, Durachinsky was using malware to secretly invade the home and privacy of scores of unsuspecting individuals, covertly turning on their computers' cameras and microphones to surveil and record them during their most private moments. Indeed, Durachinsky used his malware to secretly produce child pornography and illicit images from unknowing children. See Bradley, 488 F. App'x at 104 ("we note that the government's interest in deterring the production and dissemination of child pornography is significant.")

Third, "the governmental interest in protecting evidence from destruction is particularly high where digital evidence is involved, because such evidence is inherently ephemeral and easily destructible." Id. (citing United States v. Abbell, 963 F. Supp. 1178, 1199 (S.D. Fla. 1997) ("computer evidence is particularly vulnerable . . . to tampering or destruction through error")); see also United States v. Knowles, 207 F. Supp. 3d 585, 604 (D.S.C. 2016) (compiling cases for the proposition that "[c]ourts routinely allow warrantless seizures of laptop computers and other digital media containing child pornography under the exigent circumstances doctrine, because of 'the fragile and easily destructible nature of the digital evidence at issue.'"). The evidence at risk for destruction here also included evidence of the identities of the victims in this

case. Seizing and protecting this evidence allowed the government to properly identify and notify victims while discovering the true size and scope of defendant's criminal actions.

b. Individual Interest

The Sixth Circuit compares the strength of the government's interest in preserving the evidence at issue to the impact on defendant's interest. Saddler, 498 F. App'x at 529 (quoting Plavcak, 411 F.3d at 664.) Here, it is not disputed that Durachinsky's parents invited the FBI into their home and pointed out Durachinsky's laptop to the FBI. (R. 63: Motion to Suppress, PageID 240, 262). Once Durachinsky's parents identified his laptop, the FBI promptly seized it and obtained a warrant (within six hours) before searching the laptop.

Because the FBI "seized" defendant's "computer but did not search it until [it] had acquired a search warrant, the initial seizure affected only [defendant's] possessory interest in the laptop and did not implicate a privacy interest." Bradley, 488 F. App'x at 104 (citing Segura v. United States, 468 U.S. 796, 810 (1984)). "Courts have considered this lesser interference as a factor when upholding warrantless seizures." Id. (compiling cases). In addition, the Sixth Circuit has suggested that unlike luggage-seizures, seizure of computers do not impinge on the "liberty interests of the person from whom the property was seized" because they do not interfere with their freedom of movement or travel. Id. at 104-05 ("although the Fourth Amendment protects individuals from unreasonable interference with their possessory interests, in deciding what is reasonable, interference with possessory interests may well be less significant that interference with other rights.").

As in Bradley and Saddler, Durachinsky seems to suggest that the seizure was unreasonable because an agent could have stayed at the residence to secure the premises and/or the computer while the search warrant was obtained. (R. 63: Motion to Suppress, PageID 246-47). But both Bradley and Saddler rejected that argument, noting "the Fourth Amendment does

not require officers to engage in the least intrusive search or seizure; it only requires a reasonable alternative." Saddler, 498 F. App'x at 531 (citations omitted); Bradley, 488 F. App'x at 106. Bradley went on to quote United States v. Sharpe, 470 U.S. 675 (1985) for the proposition that

> A creative judge engaged in post hoc evaluation of police conduct can almost always imagine some alternative means by which the objectives of the police might have been accomplished. But the fact that the protection of the public might, in the abstract, have been accomplished by less intrusive means does not, itself, render the search unreasonable. The question is not simply whether some other alternative was available, but whether the police acted unreasonably in failing to recognize or to pursue it.

Id. at 686-87.

As the Court in Bradley noted, it is not obvious that leaving an officer to stand guard in order to prevent the defendant from entering his residence or accessing his laptop is less intrusive or more reasonable. Bradley, 488 F. App'x at 105 (noting that if an officer "had remained on the premises to prevent Bradley from interfering with the computer, that, too, would have implicated Fourth Amendment concerns."); cf. United States v. Hardin, 539 F.3d 404, 444 (6th Cir. 2008) (**"**both an internal securing and a perimeter stakeout interfere to the same extent with the possessory interests of the owners") (quoting Segura, 468 U.S. at 811).

In this case, Durachinsky had indicated that he was coming to the residence "with some [unidentified] friends." (R. 63-2: Exhibit B to Defendant's Motion to Suppress, PageID 314-15). Thus, there would have been safety concerns associated with leaving an FBI agent to stand guard at the residence in the middle of the night. Moreover, because the residence at issue belonged to and was inhabited by Durachinsky's parents, leaving an officer at the residence would have disturbed Durachinsky's parents, without any real benefit to Durachinsky, who would not have been permitted to touch his laptop in any event. Finally, given that the warrant was drafted, reviewed, and signed between 11:00 p.m. and 4:40 a.m., leaving an officer at the Durachinsky's

house would have required Durachinsky's parents to either stay up all night, or leave the officer unsupervised in their home—clearly a more intrusive and less reasonable result.[8]

In short, the strong governmental interests in this case outweigh the defendant's possessory interest.

4. Investigators diligently sought a warrant to search the laptop.

In McArthur, the Supreme Court observed that after seizing the defendant's home, officers diligently sought a warrant. See McArthur, 531 U.S. at 337 ("time period was no longer than reasonably necessary for the police, acting with diligence, to obtain the warrant"). Here too, investigators diligently sought and obtained a warrant.

Indeed, the warrantless seizure of Durachinsky's laptop lasted under six hours. "[D]urations longer than this have been upheld without controversy." United States v. Respress, 9 F.3d 483, 488 (6th Cir. 1993) (finding that "ten hours . . . was not an unreasonable length of time for preparing an affidavit, submitting it to a magistrate, having it reviewed, and getting the warrant issued."); Bradley, 488 F. App'x at 106 (finding warrantless seizure of laptop that lasted 26 hours to be reasonable); Saddler, 498 F. App'x at 531 (finding warrantless seizure of safe that lasted 22 hours to be reasonable); see also United States v. Van Leeuwen, 397 U.S. 249, 253 (1970) (upholding 29-hour detention of mailed package given unavoidable delay in obtaining warrant and minimal nature of intrusion); United States v. Mayomi, 873 F.2d 1049, 1054 (7th Cir. 1989) (upholding 48-hour detention of mailed packages, noting that privacy interest was not

[8] While the Court in Bradley noted that "in hindsight we *could* recognize that the better path was to seek a warrant immediately, leaving an officer behind to prevent damage to the laptop or the evidence it contained," the Court did not explain why, even in hindsight, that "could" be the "better path." Id. (emphasis added). But even if in "hindsight," that was the better path in Bradley, it would not have been the better path here for the reasons discussed above.

prematurely disturbed). It is also noteworthy that those 5+ hours took place during the hours of 11:00 p.m. to 4:40 a.m.—late night hours when most people are less likely to need use of their computer.

In sum, the temporary seizure of Durachinsky's laptop under the exigent circumstances exception to the warrant requirement was proper and Durachinsky's motion should be denied.

B. THE UNITED STATES ACTED IN GOOD FAITH

Even if the temporary seizure of Durachinsky's laptop is determined to have been improper, the fruits of the seizure will not be suppressed if the United States acted in good faith. In Herring v. United States, the Supreme Court laid out five key principles related to the exclusionary rule and good faith analysis. 555 U.S. 135 (2009). The Court noted: (1) "the exclusionary rule is not an individual right and applies only where it 'result[s] in appreciable deterrence;'" (2) "the benefits of deterrence must outweigh the costs;" (3) "the extent to which the exclusionary rule is justified by these deterrence principles varies with the culpability of the law enforcement conduct;" (4) "the pertinent analysis of deterrence and culpability is objective, not an inquiry into the subjective awareness of arresting officers;" and (5) "when police mistakes are the result of negligence . . . rather than systemic error or reckless disregard of constitutional requirements, any marginal deterrence does not 'pay its way.'" Herring, 555 U.S. at 141-48; see also Davis v. United States, 564 U.S. 229, 240 (2011) ("Police practices trigger the harsh sanction of exclusion only when they are deliberate enough to yield meaningfu[l] deterrence, and culpable enough to be 'worth the price paid by the justice system.'") (citations omitted). Thus, unlawfully obtained evidence should not be suppressed "when the police act with an objectively 'reasonable good-faith belief' that their conduct is lawful." Davis, 564 U.S. at 232.

In the present case, the United States objectively acted in good faith. Law enforcement—after consulting with Department of Justice attorneys, and believing that destruction of key

evidence was imminent based on multiple public disclosures on January 18, 2017—seized the laptop that same day and obtained a signed warrant to search the laptop in the middle of the night and within less than six hours of the seizure. In the event that this seizure was somehow not covered by the exigent circumstances doctrine, it was executed in good faith and was "close enough to the line of validity" to make the conduct objectively reasonable. See, e.g., United States v. Fugate, 599 F. App'x 564, 567 (6th Cir. 2014) ("officer was not culpable because the warrantless entry into the yard was 'close enough to the line of validity' to make his conduct objectively reasonable"); United States v. McClain, 444 F.3d 556, 566 (6th Cir. 2005) (suppression properly denied under "good faith" doctrine where court found "no evidence that the officers knew they were violating the Fourth Amendment by performing a protective sweep of the home."). Because this seizure did not involve anything near "systemic error or reckless disregard of constitutional requirements, any marginal deterrence does not 'pay its way.'" Herring, 555 U.S. at 141-48.

C. THE INEVITABLE DISCOVERY DOCTRINE APPLIES

In addition, the inevitable discovery doctrine applies to this seizure. "[T]he inevitable discovery exception to the exclusionary rule applies when the government can demonstrate *either* the existence of an independent, untainted investigation that inevitably would have uncovered the same evidence or other compelling facts establishing that the disputed evidence inevitably would have been discovered." United States v. Keszthelyi, 308 F.3d 557, 574 (6th Cir. 2002) (internal quotation marks and citations omitted) (emphasis in original). "The government can satisfy its burden by showing that routine procedures that police would have used regardless of the illegal search would have resulted in the discovery of the disputed evidence." Id. "Although the application of the doctrine requires some speculation about how events would have transpired absent any illegality, 'we must keep speculation at a minimum by

focusing on demonstrated historical facts capable of ready verification or impeachment.'" United States v. Stamper, 91 F. App'x 445, 458 (6th Cir. 2004) (quoting Keszthelyi, 308 F.3d at 574). "The exception requires the district court to determine, viewing affairs as they existed at the instant before the unlawful search, what would have happened had the unlawful search never occurred." United States v. Kennedy, 61 F.3d 494, 498 (6th Cir. 1995) (citation omitted).

In the present case, had the exigent seizure never occurred, the United States would have prepared a warrant and seized the laptop pursuant to the warrant. That the United States would have sought a warrant is a "demonstrated historical fact[s] capable of ready verification" because, prior to visiting the Durachinsky residence, the United States contacted the magistrate judge on duty to let him know that it would be seeking a warrant later that night and received instructions from the magistrate judge on how to reach him at home (which is one reason the FBI was able to obtain a warrant so quickly at 4:40 a.m.). See Kennedy, 61 F.3d at 498; see also United States v. Vanaman, 12 F. App'x 222, 231–32 (6th Cir. 2001) (inevitable discovery doctrine applied to warrantless search where "the mechanism to obtain the search warrant was begun before the alleged police misconduct"); United States v. Souza, 223 F.3d 1197, 1205–06 (10th Cir. 2000) (applying inevitable discovery doctrine to warrantless search where agent "took steps to alert his office that he would be coming back to prepare a warrant for the package and made sure that the affidavit form would be ready when he got back to his office."); United States v. Lewis, 672 F. Supp. 2d 827, 835 (S.D. Ohio 2009) (inevitably discovery doctrine applied where the evidence allegedly improperly seized "would have been discovered through lawful

means very shortly thereafter, namely, through the warrant for which [law enforcement] had already applied.").[9]

Further, for the reasons discussed in Section A(1) above, prior to the FBI's visit to the Durachinsky residence, the United States already had probable cause to believe that evidence of a crime would be found on digital devices within the residence. See United States v. Taylor, 248 F.3d 506, 514 (6th Cir. 2001) (affirming denial of motion to suppress under the "inevitable discovery doctrine" where "before the officers conducted the protective sweep, they had probable cause to obtain a search warrant."); see also United States v. Dessesaure, 429 F.3d 359, 369–70 (1st Cir. 2005) (evidence admissible because search warrant was obtained on basis of facts gathered legally prior to illegal search).

Had the January 18, 2017, seizure never occurred, the United States believes that Durachinsky may have destroyed some or all of the evidence seized. Public policy dictates, however, that it is no defense to the inevitable discovery doctrine, that had the seizure never occurred, defendant may have later deleted or destroyed the evidence in an effort to conceal his criminal conduct. See, e.g., United States v. Husband, 226 F.3d 626, 640 (7th Cir. 2000) ("The exclusionary rule is not designed to reward the destruction of evidence."); United States v. Jones, 214 F.3d 836, 838 (7th Cir. 2000) (defendant could not argue that he would have destroyed the evidence but for the officer's unreasonable manner of entry); see also Segura, 468 U.S. at 813-16

[9] To the extent that United States v. Griffin, 502 F.2d 959 (6th Cir. 1974) and United States v. Buchanan, 904 F.2d 349 (6th Cir. 1990) suggest that the fact that the police were in the process of obtaining a warrant is not relevant to the inevitable disclosure doctrine, the holding of cases have subsequently been limited by the Sixth Circuit to cases where "the police intentionally took a shortcut in an attempt to bypass the Fourth Amendment warrant requirement—in effect, the police conducted an illegal search to determine whether it would be worthwhile to obtain a search warrant." Kennedy, 61 F.3d at 499 n.2. That is not the case here.

(when deciding whether discovery was "inevitable," courts must assume that suspects behave lawfully).

In arguing the inevitable discovery doctrine does not apply, Durachinsky relies upon three Sixth Circuit cases—Haddix, Quinney, and Bowden—all of which stand for the unremarkable proposition that the inevitable disclosure doctrine does not apply merely because the government could have obtained a warrant but elected not to get one. See, e.g., United States v. Bowden, 240 F. App'x 56, 63 (6th Cir. 2007) (citing Haddix for the proposition that "[d]oubtless, the inevitable-discovery doctrine does not permit police, who have probable cause to believe a home contains contraband, to enter a home illegally, conduct a warrantless search and escape the exclusionary rule on the ground that the 'police could [have] obtain[ed] a warrant yet cho[ ]se not to do so.'). The United States agrees that allowing the police to engage in such conduct would eviscerate the warrant requirement. At the same time, if law enforcement were not permitted to temporarily seize evidence as part of a good faith basis to prevent the imminent destruction of such evidence, it would eviscerate the exigent circumstances exception (as that exception is applied to prevent the destruction of evidence). See King, 563 U.S. at 461–62 ("a rule that precludes the police from making a warrantless entry to prevent the destruction of evidence whenever their conduct causes the exigency would unreasonably shrink the reach of this well-established exception to the warrant requirement.")

Here, the inevitable disclosure doctrine applies, among other reasons, because unlike in Haddix, Quinney, and Bowden, (1) "the mechanism to obtain the search warrant was begun before the alleged police misconduct"; (2) the FBI had a specific and good faith basis to believe exigent circumstances existed and executed the seizure in a reasonable manner; and (3) a warrant was obtained late at night, within six hours of the seizure, and before the laptop was searched.

Durachinsky also suggests that the independent source cannot apply because the warrant affidavit includes observations from Durachinsky's home, which he claims were obtained unlawfully. Even if the home observations were unlawful, however, the warrant would not be invalid. The independent-source exception to the exclusionary rule permits the admission of "evidence initially discovered during, or as a consequence of, an unlawful search, but later obtained independently from activities untainted by the initial illegality." Murray v. United States, 487 U.S. 533, 537 (1988). When a warrant-based search follows an illegal search, "the search pursuant to warrant [must] in fact [have been] a genuinely independent source of the information and tangible evidence at issue." Id. at 542. A warrant-based search is not independent if the "decision to seek the warrant was prompted by what [the officers] had seen during the [illegal search], or if information obtained during that [illegal search] was presented to the Magistrate and affected his decision to issue the warrant." Id. (footnote omitted). See also United States v. Jenkins, 396 F.3d 751, 760 (6th Cir. 2005) (holding that where a warrant affidavit includes tainted information, a reviewing court excises the tainted evidence and determines whether the remaining untainted evidence establishes probable cause). Here, even if the home observations in the affidavit were unlawful, the fruits of the warrant would not be suppressed under Murray and Jenkins.

First, investigators were already in the process of seeking the warrant before they visited Durachinsky's home, so it is clear that their decision to seek the warrant was not prompted by anything at the home. Second, as discussed previously, the United States had probable cause to search the home before it arrived there, and these facts were included in the affidavit. Thus, when any potentially tainted information is removed from the affidavit, probable cause remains.

IV. CONCLUSION

For the reasons discussed above, Durachinsky's motion to suppress should be denied.

Respectfully submitted,

JUSTIN E. HERDMAN
United States Attorney

By: /s/ Brian L. Levine

Brian L. Levine (DC: 480216)
Senior Counsel
United States Department of Justice
1301 New York Avenue, Suite 600
Washington, DC 20005
(202) 616-5227
(202) 514-6113 (facsimile)
Brian.Levine@usdoj.gov

/s/ Daniel J. Riedl

Daniel J. Riedl (OH: 0076798)
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3669
(216) 685-2378 (facsimile)
Daniel.Riedl@usdoj.gov

/s/ Om M. Kakani

Om M. Kakani (NY: 4337705)
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3756
(216) 522-8355 (facsimile)
Om.Kakani@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on this 13th day of May, 2019, a copy of the foregoing document was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. All other parties will be served by regular U.S. Mail. Parties may access this filing through the Court's system.

/s/ Daniel J. Riedl
Daniel J. Riedl
Assistant U.S. Attorney